UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/614,487	07/11/2000	Eugene Amdur	DSC-003	2054

7733 7590 02/11/2004

WALKER & JOCKE, L.P.A.
231 SOUTH BROADWAY STREET
MEDINA, OH 44256

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/614,487	AMDUR ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *7/11/2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-16 rejected under 35 U.S.C. 103(a) as being unpatentable over Mitsutaka, Japanese Patent #11-98134-A(hereafter referred to as '134) in view of Bruce Schneier, "Applied Cryptography" (hereafter referred to as Schneier).

As to Claim 1, '134 teaches a method for authenticating target data comprising:

- Data forwarding computer... / Computer which provides WWW service (Section 7, Line 1 et seq., '134); Sends to user terminal as Cookie (Section 6, Line 15 et seq., '134)
- Computer usable medium... / program store medium (Section 1, Line 1 et seq., '134)
- Generating an encrypted digital signature... / Digital signature combined with encryption of cookie (Section 6, Line 4 et seq., '134)
- Computer readable program code means... / Stored program for implementing method (Section 1, Line 2 et seq., '134)
- Public key encryption system... / Fast date encypherment algorithm which is procedure public (Section 10, Line 5 et seq., '134)

- Private key in dynamic memory... / Encryption key maintained on memory (Section 14, Line 4 et seq., '134)
- Generate a digital signature for the target data... / Adding digital signature to cookie (Section 6, Line 4 et seq., '134)
- Encrypt the digital signature... / Combines with encryption of Cookie (Section 6, Line 7 et seq., '134)
- Forward the target data... / Sends to user terminal as Cookie (Section 6, Line 15 et seq., '134)

'134 does not explicitly teach to store the public key in a centralized database available to the set of recipient computers. Schneier teaches the use of a centralized database where public keys may be stored and retrieved (Page 185,"Public-Key Key Management", Line 6 et seq., Schneier). It would have been obvious to a person skilled in the art at the time of invention to incorporate the storage and retrieval of public keys from a centralized database into the invention as disclosed in '134. One of ordinary skill in the art would have been motivated to incorporate this method of key management because it is very well known in the art as an alternative method of key management implemental on any client-server network.

As to claim 2:

'134 teaches a method for authenticating target data by means of a public-key encryption system and storing the encryption key in memory. '134 does not explicitly teach the means to obtain a replacement key after a restart. The examiner takes official

notice as to the means to obtain a replacement key after restart. It is well known in the art that many computer systems use a volatile dynamic memory as their primary memory, and so the key stored in memory would be erased upon restart. It would have been obvious to a person of ordinary skill in the art at the time of invention to obtain a replacement key on after restart. One of ordinary skill in the art would have been motivated to obtain a replacement key on after restart because the invention disclosed in '134 implemented on such a system would necessitate a means to obtain a replacement key after a restart.

As to claim 3:

'134 teaches a method for authenticating target data by means of a public-key encryption system. '134 does not teach all the specific key management techniques it employs, including the key lifecycle time. Schneier discloses some of the well known advantageous key lifecycle strategies:

- Determine an elapsed time... / There must be a policy that determines the permitted lifetime of a key (Page 184, Line 3 et seq., Schneier)
- Purge each public key... / old keys must be destroyed (Section 8.11, Line 1 et seq., Schneier)
- Longer than the elapsed time... / There must be a policy that determines the permitted lifetime of a key (Page 184, Line 3 et seq., Schneier)

It would have been obvious to a person of ordinary skill in the art at the time of invention to implement '134 with the key lifecycle strategies as disclosed in Schneier. One of

ordinary skill in the art would have been motivated to implement these strategies because they are very well known in the art as advantageous security policies used on a variety of platforms.

As to claim 4 and 5:

The combination of inventions as described above discloses a method for authenticating target data by means of a public-key encryption system using a centralized database to store keys associated with various users and their corresponding cookies. Not specifically stated is to use a unique identifier to reference the data/keys. The examiner takes official notice as to the use of a look-up table database implementation for this purpose. It would have been obvious to a person of ordinary skill in the art at the time of invention to use a look-up table database implementation for the referencing of data/keys. One of ordinary skill in the art at the time of invention would have been motivated to use a look-up table database implementation for the referencing of data/keys because the look-up table database is very well known and commonly used in the art as a database structure for referencing data based by means of a unique key.

As to claims 6-10, they correspond to claims 1-5. Accordingly, they are rejected by the references listed above.

As to claim 11, it recites a combination of previously rejected claim limitations further comprising:

- Client-server computer network... / Sent to www browser (Client) from WWW server (Section 3, Line 1 et seq., '134)
- Generate a cookie... / Cookie Generation (Section 13, Line 7 et seq., '134)
- Communicate with a second one of the set of server computers... / Get public key from a centralized database (Page 185,"Public-Key Key Management", Line 3 et seq., Schneier)
- Decrypt the digital signature... / Verifies digital signature (Section 13, Line 11 et seq., '134)
- Authenticate the cookie... / Digital signature is verified (Section 8, Line 4 et seq., '134)

The combination of inventions does not explicitly disclose the function of Cookies in their entirety. The means to provide identifying data is deemed to be inherent to the invention as disclosed above as "Cookies are used to Identify users" (Page 129, "cookie", Microsoft Computer Dictionary).

As to claims 12 and 13, they recite a combination of limitations of previously rejected claim, and therefore fail to distinguish over them accordingly. See above for the specifics of the rejection.

As to claims 14 - 16, they recite a combination of limitations of previously rejected claim, and therefore fail to distinguish over them accordingly. See above for the specifics of the rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703) 305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306 Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100